

~~TOP SECRET//COMINT//ORCON,NOFORN~~

UNITED STATES

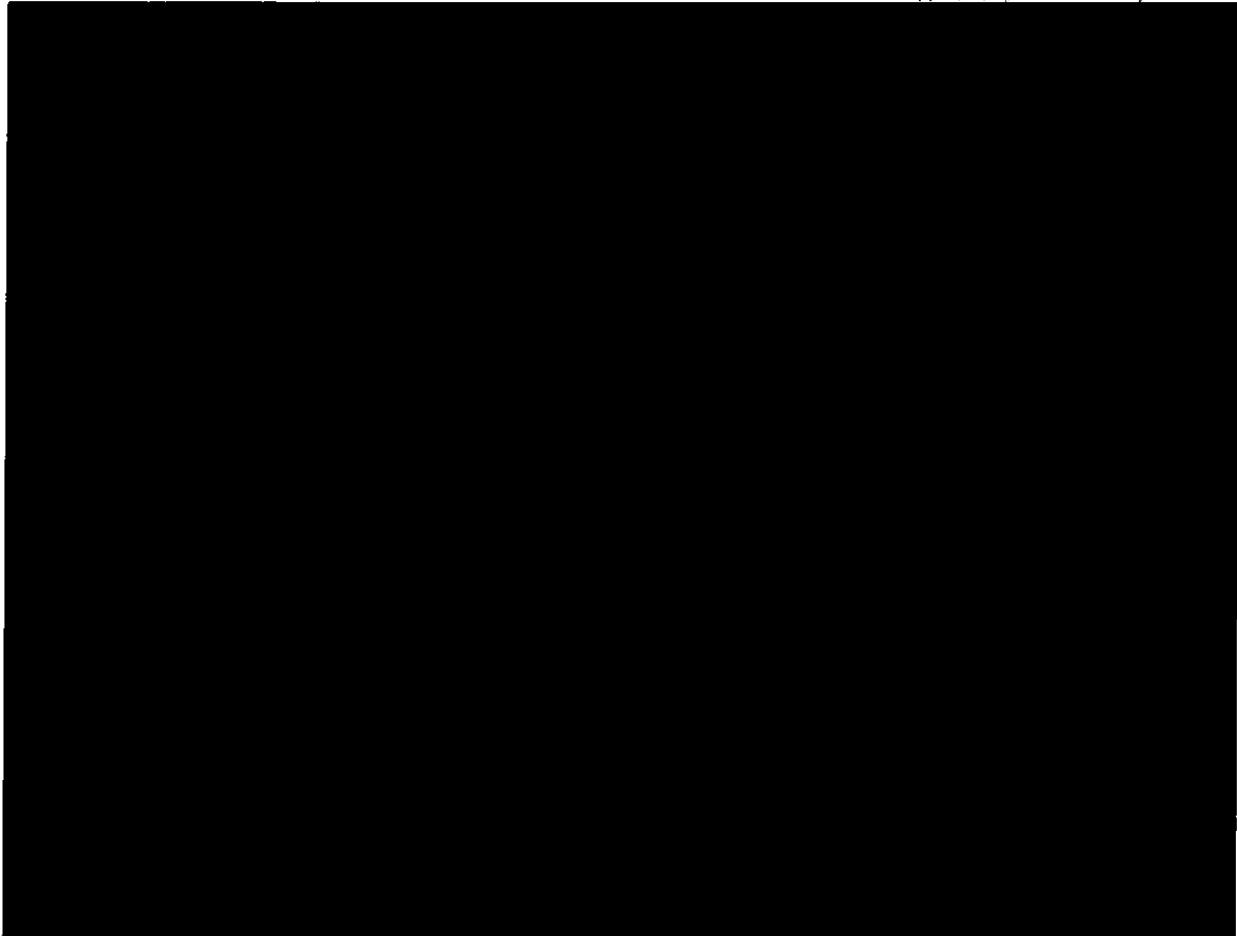
FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

SURVEILLANCE COURT

2011 NOV 22 PM 5:28

LEAHN FLYNN HALL



GOVERNMENT'S RESPONSE TO THE COURT'S  
BRIEFING ORDER OF OCTOBER 13, 2011

THE UNITED STATES OF AMERICA, through the undersigned Department of  
Justice attorney, respectfully submits the following response to the Court's Briefing  
Order of October 13, 2011. ~~(S//OC,NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Classified by: Tashina Gauhar, Deputy Assistant  
Attorney General, NSD, DOJ  
Reason: 1.4(c)  
Declassify on: 22 November 2036

~~TOP SECRET//COMINT//ORCON,NOFORN~~

The Court's Briefing Order of October 13, 2011, in the above-captioned matters (hereinafter "October 13 Briefing Order") enumerated six issues to be addressed by the Government. Items 1. and 2. in the October 13 Briefing Order are addressed together starting on page 3 below; responses for items 3. through 6. begin on page 39. (S)

As an initial matter, as this Court is aware, amended section 702 minimization procedures for the National Security Agency (NSA) were adopted by the Attorney General and approved by the Attorney General and Director of National Intelligence for immediate use on October 31, 2011; that same day the procedures were submitted to the Court for review. NSA's amended section 702 minimization procedures provide, *inter alia*, that "[a]ll Internet transactions may be retained no longer than two years from the expiration date of the certification authorizing the collection in any event." See, e.g., Amendment to DNI/AG 702(g) Certification [REDACTED] Ex. B, filed Oct. 31, 2011, § 3(c)(2) (hereinafter "2011 Amended NSA Minimization Procedures"). In the past, NSA has tried to maintain consistency of its minimization procedures across acquisitions pursuant to multiple certifications. NSA is unable to apply in full the 2011 Amended NSA Minimization Procedures to information acquired prior to October 31, 2011, for technical reasons primarily related to its inability to segregate certain previously collected categories of information in accordance with section 3(b)(5)a. of the amended

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

procedures.<sup>1</sup> Nevertheless, in furtherance of maintaining consistency across data acquired through its upstream collections, and as described in greater detail below, NSA is taking steps to age off of its systems Internet transactions that were collected through its upstream collection platforms pursuant to Docket Nos. [REDACTED] the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (Aug. 5, 2007) (hereinafter PAA), and certifications issued under section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. §§ 1801, *et seq.* (hereinafter FISA or "the Act") where such authorizations expired more than two years ago. NSA anticipates that it will complete this age-off process no earlier than March 2012. ~~(TS//SI//NF)~~

1. An analysis of the application of Section 1809(a) to each of the three different statutory schemes under which Internet transactions were acquired without the Court's knowledge. ~~(TS//SI//NF)~~
2. The extent to which information acquired under Section 1881a, the PAA, and Docket Nos. [REDACTED] falls within the criminal prohibitions set forth in Section 1809(a). ~~(S)~~

The Government responds to these two items as follows: ~~(S)~~

---

<sup>1</sup> It is for this reason that NSA has not sought to amend prior certifications to permit the use of the 2011 Amended NSA Minimization Procedures to information acquired under those certifications. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

I. The Application of Section 1809 to the Government's Acquisitions Pursuant to Section 1881a, the PAA, and Docket Nos. [REDACTED] (S)

A. Section 1809 is a Criminal Statute Designed to Address Intentional Violations of the Law (S)

As acknowledged earlier this year, the Government concluded that its prior representations to the Court regarding the steps NSA must take in order to acquire single, discrete communications to, from, or about a tasked selector did not fully explain all of the means by which such communications are acquired through NSA's upstream collection techniques. The Government submits that that oversight, although regrettable, does not support a finding that the Government intentionally engaged in unauthorized electronic surveillance, thus implicating a criminal statute. Section 1809 by its terms imposes criminal sanctions (including imprisonment and a substantial fine) on an individual who intentionally engages in unauthorized electronic surveillance or uses or discloses the fruits of unauthorized electronic surveillance.<sup>2</sup> Congress did not intend these stringent penalties to apply to intelligence professionals who, in good faith, reasonably believed that they were acquiring foreign intelligence information in conformity with authorizations by this Court or by the Attorney General and Director of National Intelligence. ~~(TS//SI//NF)~~

Section 1809(a) criminalizes "intentionally (1) engag[ing] in electronic surveillance under color of law, except as authorized by [statute] . . . ; or (2) disclos[ing]

---

<sup>2</sup> Section 1810 of FISA exposes an individual who violates section 1809 to substantial civil penalties. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

or us[ing] information obtained under of color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by [statute]." 50 U.S.C. § 1809(a). Section 1809 provides a complete defense for law enforcement and investigative officers engaged in official surveillance "authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction." *Id.* § 1809(b). Accordingly, by its terms section 1809(a) is violated only where there is intentional conduct and unauthorized electronic surveillance is involved. ~~(S)~~

FISA's inclusion of criminal sanctions reflects a balance between competing priorities. On the one hand, the threat of criminal sanctions reinforces FISA's central edict: before engaging in electronic surveillance, Government agents must obtain the necessary statutory authorization -- typically (though not always) by securing advance judicial approval. On the other, those agents who in good faith obtain and effectuate authorization under the FISA framework are thereby shielded from civil and criminal liability. FISA's proponents stressed that far from chilling lawful intelligence collection, the bill's clear delineation of the scope of criminal liability actually serves to *protect* law-abiding Government agents:

[I]ndividual intelligence agents will know to the letter what is required of them. They will know that what they do pursuant to a warrant is lawful. And they will be protected in the future against criminal prosecutions and civil suits arising from the surveillance as long as they do not exceed their lawful authority.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

*Foreign Intelligence Surveillance Act: Hearing on H.R. 7308 Before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice, House Committee on the Judiciary, 95th Cong. 111 (1978) (statement of Rep. Mazzoli).* To that end, "[t]he word 'intentionally' was carefully chosen. It [was] intended to reflect the most strict standard for criminal culpability. . . . The Government would have to prove beyond a reasonable doubt that the . . . [conduct] was engaged in with a conscious objective or desire to commit a violation." H.R. Rep. No. 95-1283, pt. 1, at 97 (1978) (quotation omitted). In other words, "intentionally" in the context of section 1809 means not only that an individual intentionally undertook electronic surveillance, but undertook electronic surveillance with the knowledge and intention to violate the requirements of FISA. As noted in the Government's Response to the Court's Briefing Order of May 9, 2011, "[b]ased upon discussions between responsible NSA officials and the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) and DOJ and ODNI's review of documents related to this matter, DOJ and ODNI have not found any indication that there was a conscious objective or desire to violate the authorizations here." Government's Response to the Court's Briefing Order of May 9, 2011, Docket Nos. [REDACTED], filed June 1, 2011, at 32 n.27 (hereinafter "June 1 Submission"). In addition, DOJ and ODNI have not found any indication of a conscious objective or desire to violate the authorizations under the PAA or Docket Nos. [REDACTED] (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

The enacted version of section 1809 contrasts markedly with a criminal-sanctions provision in a draft bill that would have swept more broadly. The earlier proposal would, among other things, have criminalized intentionally "violat[ing] ... any court order pursuant to this title." H.R. Rep. No. 95-1283, pt. 1, at 96-97 (discussing predecessor bill). Criminalizing all manner of FISA violations "generated considerable debate" and was suggested to have a "deleterious effect on the morale of intelligence personnel." *Id.* at 96. The "any order" language was ultimately stricken from the final bill enacted by Congress. In limiting FISA's criminal penalties to instances in which the Government had failed to obtain prior authorization or intentionally exceeded the boundaries of the authorization obtained, Congress made clear that it envisioned section 1809 as a narrowly tailored sanction, not a comprehensive framework for remedying all manner of Government errors in the course of obtaining or effectuating FISA authorities. (S)

Given its underlying purpose, the Government respectfully suggests that section 1809 does not provide the appropriate framework for cases in which the "surveillance, though based on an erroneous factual premise, was authorized by and conducted pursuant to an order issued by the FISC." Note, *The Notice Problem, Unlawful Electronic Surveillance, and Civil Liability under FISA*, 61 U. Miami L. Rev. 393, 427 (2007) (arguing that although this limitation of section 1809 was "appropriate for criminal liability," FISA should be amended to provide civil liability in such circumstances). So

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

understood, section 1809 accords with other criminal offenses that hinge on the absence of valid authorization. For example, in *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004), the Ninth Circuit construed "the meaning of the word 'authorized' in section 2701" of the Stored Communications Act (SCA), 18 U.S.C. § 2702. The defendant in *Theofel* had obtained access to communications by serving a "patently unlawful" subpoena on a third party. *Id.* At issue was whether compliance with that flawed subpoena constituted valid consent -- i.e., qualified as an "authorized" disclosure under the SCA. ~~(S)~~

Holding that the answer depended on whether the authorization was procured in "bad faith," the Court of Appeals explained:

Because the Stored Communications Act defines a criminal offense and includes an explicit *mens rea* requirement, see 18 U.S.C. § 2701(a)(1), we do not think a defendant can be charged with constructive knowledge [of the authorization's invalidity] on a showing of mere negligence. Rather, the defendant must have consciously procured consent [i.e., "authorization"] through improper means. In this case, the magistrate found that defendants had acted in bad faith. That is enough to charge them with knowledge of [the third party's] mistake. See Black's Law Dictionary 139 (6th ed. 1990) (defining "bad faith" as "not simply bad judgment or negligence, but . . . conscious doing of a wrong because of dishonest purpose or moral obliquity").

*Id.* at 1074 n.2. In addition to recounting the defendant's "bad faith" and "constructive knowledge" of the subpoena's invalidity, the decision stressed that "[a]llowing consent procured by a known mistake to qualify as a defense would seriously impair the statute's operation." *Id.* at 1074. However, for the reasons discussed herein, the

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

Government submits that the orders of the Court in the four authorities at issue here were not "procured by a known mistake." ~~(S)~~

The Government submits that the same considerations exclude from criminal liability under section 1809 instances in which judicial approval and authorization of the Director of National Intelligence and the Attorney General were obtained in good faith, premised on incomplete descriptions of how the acquisitions were to be conducted. ~~(TS//SI//NF)~~

B. The Authorizations Remain Valid Despite the Government's Incomplete Description of the Technical Means of Acquisition ~~(S)~~

Congress intended that the "criminal penalties for intelligence agents under [FISA] should be essentially the same as for law enforcement officers under title 18." H.R. Conf. Rep. No. 95-1720, at 33 (1978). Therefore, the law-enforcement context provides instructive guidance with respect to the scope of what should qualify as intentional unauthorized surveillance for purposes of section 1809(a)(1). Provided it was obtained in good faith, a valid authorization to conduct law-enforcement surveillance is not rendered "void" or "invalid" because it was premised on a factual error or misstatement. ~~(S)~~

Under case law developed in the suppression context, it has long been settled that the Government's "[i]nnocent mistakes or negligence alone are insufficient to void a warrant." *United States v. Palega*, 556 F.3d 709, 714 (8th Cir. 2009) (citing *Franks v.*

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

*Delaware*, 438 U.S. 154, 171) (1978)).<sup>3</sup> Recognizing that everyone -- including the agents who serve the Government -- will at times commit errors, the Supreme Court has emphasized, in a variety of circumstances, "the need to allow some latitude for honest mistakes." *Maryland v. Garrison*, 480 U.S. 79, 87 (1987); see also *Brinegar v. United States*, 338 U.S. 160, 176 (1949) (emphasizing that "room must be allowed for some mistakes on [the Government's] part"). ~~(S)~~

In the three decades since *Franks*, it has become hornbook law that a discovery of a good faith misstatement or omission<sup>4</sup> in the application for a warrant -- even one that is material -- does not transform an authorized search into an unauthorized one. See e.g., *Chism v. Washington State*, No. 10-35085, \_\_\_ F.3d \_\_\_, 2011 WL 5304125, at \*16 (9th Cir. Nov. 7, 2011) ("It is well established that omissions and misstatements resulting from negligence or good faith mistakes will not invalidate an affidavit which on its face

---

<sup>3</sup> The decision in *Franks* came down in June 1978, just prior to FISA's enactment. But the core holding of *Franks* was anticipated by many courts. See, e.g., *United States v. Marihart*, 492 F.2d 897, 900 n.4 (8th Cir. 1974) ("We agree with the Seventh Circuit that completely innocent misrepresentation should not support suppression even if material."). The Second Circuit has suggested that "FISA orders should be governed by the principles set forth in *Franks v. Delaware*." *United States v. Duggan*, 743 F.2d 59, 77 n.6 (2d Cir. 1984). Under the Second Circuit's standard, the fact of a negligent misstatement in a FISA application is not grounds for suppression -- or even an evidentiary hearing -- on the issue of whether the surveillance was properly authorized. To warrant a hearing, the court explained, a suppression motion asserting that the Government's surveillance was not authorized by FISA "would be required to make 'a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included' in the application and that the allegedly false statement was 'necessary' to the FISA judge's approval of the application." *Id.* (quoting *Franks*, 438 U.S., at 155-156). ~~(S)~~

---

<sup>4</sup> Although *Franks* itself was concerned with the issue of Government misstatements, it is widely accepted that its "reasoning . . . logically extends . . . to material omissions." *United States v. Johnson*, 696 F.2d 115, 118 n.21 (D.C. Cir. 1982) (quoting 2 W. LaFare, Search and Seizure, § 4.4 (Supp. 1982)). ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

establishes probable cause.") (quotation omitted); *United States v. Andrews*, 577 F.3d 231, 238-39 (4th Cir. 2009) ("In challenging a search warrant on the theory that the officer's affidavit omitted material facts with the intent to make, or in reckless disregard of whether they thereby made, the affidavit misleading, the defendant must show (1) that the officer deliberately or recklessly omitted the information at issue and (2) that the inclusion of this information would have defeated probable cause.") (quotation and citation omitted). The appropriate inquiry looks to the Government's good faith in submitting the application, and the fact that an error may be attributable to an internal miscommunication within the Government, or to gaps in the Government's understanding, is not itself an indication of bad faith. See, e.g., *United States v. Yusuf*, 461 F.3d 374, 378 (3d Cir. 2006) (in performing the *Franks* analysis, lower court "erred by failing to recognize that government agents should generally be able to presume that information received from a sister governmental agency is accurate"); *United States v. Radtke*, 799 F.2d 298, 310 (7th Cir. 1986) (finding no "deliberate falsehood" where a police officer of one department compiled erroneous information derived from another department's investigation).<sup>5</sup> ~~(S)~~

---

<sup>5</sup> The case law "hold[s] the government accountable for statements made . . . by the affiant [and] statements made by other government employees which were deliberately or recklessly false or misleading insofar as such statements were relied upon by the affiant in making the affidavit." *United States v. Kennedy*, 131 F.3d 1371, 1376 (10th Cir. 1997). See also *United States v. Hammett*, 236 F.3d 1054, 1058-1059 (9th Cir. 2001) ("In informing Detective Bolos of the information necessary to procure the warrant, it is highly probable that there was a miscommunication between Officer Correia and Detective Bolos that led to the misstatement in the affidavit. We therefore reject the position that the warrant is invalid . . ."); *United States v. Wapnick*, 60 F.3d 948, 956 (2d Cir. 1995) (invalidation turns on whether

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

The *Franks* framework has been extended to mistakes in Title III applications. As Judge Posner has explained:

[I]f government agents execute a valid wiretap order and in the course of executing it discover it was procured by a mistake . . . the record of the conversations is admissible in evidence . . . The discovery of the mistake does not make the search unlawful from its inception.

*United States v. Ramirez*, 112 F.3d 849, 851 (7th Cir. 1997); see also *United States v. Garcia*, 785 F.2d 214, 222 (8th Cir. 1986) (applying *Franks* standard to a Title III wiretap); *United States v. Ippolito*, 774 F.2d 1482, 1485 (9th Cir. 1985) (same); *United States v. Southard*, 700 F.2d 1, 8 (1st Cir. 1983) (same). ~~(S)~~

Although the Government has not located cases applying the *Franks* standard to illegal wiretapping prosecutions (presumably because cases raising that fact pattern are rarely, if ever, prosecuted), *Franks* also delineates the scope of an "illegal search" in civil litigation under 42 U.S.C. § 1983. See, e.g., *Peet v. City of Detroit*, 502 F.3d 557, 570 (6th Cir. 2007) ("In cases involving search warrants . . . the law is clear that an officer may be held liable under 42 U.S.C. § 1983 for an illegal search . . . when the officer 'knowingly and deliberately, or with a reckless disregard for the truth' makes 'false statements or omissions that create a falsehood' and 'such statements or omissions are material, or necessary, to the finding of probable cause.'") (citing *Wilson v. Russo*, 212 F.3d 781, 786-787 (3d Cir. 2000)). When it enacted section 1809, Congress surely did not intend to

---

anyone in the government "deliberately insulat[ed] affiants from information material to the determination of probable cause") (emphasis added); *United States v. Calisto*, 838 F.2d 711, 714 (3d Cir. 1988) (same). ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

impose a less forgiving standard of *criminal liability* in the national security context than generally exists for *civil liability* in the law-enforcement context. ~~(S)~~

The Government submits that the Court should consider the latitude afforded the Government in the law-enforcement context equally appropriate for surveillance conducted under the aegis of national security investigations, in which the Government's focus will often be "less precise . . . than [surveillance] directed against more conventional types of crime." *United States v. United States District Court (Keith)*, 407 U.S. 297, 322 (1972). All of which is not to suggest that the Government bears diminished responsibility for mistakes in the record. Upon becoming aware of its failure to communicate to the Court certain salient aspects of its collection activities, the Government bore responsibility for correcting its past statements. See FISC Rule 13(a). When mistakes happen notwithstanding the Government's best efforts, they are regrettable. Nevertheless, the Government respectfully submits that the potential exposure to *criminal liability* -- and the resultant civil liability under section 1810 -- is not the appropriate means to respond to such miscommunications within the Government. ~~(S)~~

C. The Authorities at Issue ~~(S)~~

1. Section 1881a ~~(S)~~

Beneath the heading "AUTHORIZATION," section 702 in pertinent part empowers the Attorney General and the Director of National Intelligence, upon the issuance of an

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

order from this Court approving a certification and the use of targeting and minimization procedures, to "authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). Acquisitions authorized under section 702 must be conducted in accordance with targeting and minimization procedures adopted by the Attorney General and in conformity with a certification submitted to the FISC. *See* 50 U.S.C. § 1881a(c)(1). Accordingly, section 702 accords the Court a crucial role in ensuring that the Government's targeting and minimization procedures are consistent with the statutory requirements of section 702 and the Fourth Amendment to the Constitution of the United States. *See* 50 U.S.C. § 1881a(i) (providing that the FISC "shall have jurisdiction to review [the] certification . . . and the targeting and minimization procedures"). Nevertheless, while the Government cannot commence or continue acquisition without Court approval, the statute commits responsibility for "authorization" to the Attorney General and the Director of National Intelligence. ~~(TS//SI//NF)~~

Section 702 provides for two potential outcomes of judicial review, neither of which appears to vitiate a past determination of the Attorney General and Director of National Intelligence to authorize acquisitions in good faith. The first is "APPROVAL," in which event the Court "enter[s] an order approving the certification and the use . . . of the procedures for the acquisition." 50 U.S.C. § 1881a(i)(3)(A). The second is a

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

"CORRECTION OF DEFICIENCIES," in which event the Court "shall issue an order directing the Government to, at the Government's election . . . (i) correct any deficiency identified by the Court's order . . . ; or (ii) cease, or not begin, the implementation of the authorization for which such certification was submitted." 50 U.S.C. § 1881a(i)(3)(B). Notably, section 702 makes no provision for an order requiring the Government to purge information acquired under authorizations from the Attorney General and Director of National Intelligence in the event the Government chooses to discontinue its collection after receipt of a deficiency order.<sup>6</sup> ~~(S)~~

In keeping with the above, the operative certifications, and the targeting and minimization procedures adopted by the Attorney General for use with those certifications, were submitted by the Government to the FISC and approved pursuant to 50 U.S.C. § 1881a(i), albeit without provision of certain information relevant to the manner in which NSA acquires Internet transactions to, from, or about a tasked selector through its upstream collection. The Attorney General and Director of National Intelligence at all times acted in good faith in discharging their responsibilities under section 702. As the Court has already found, each prior certification contained all of the required statutory elements. *See In re DNI/AG 702(g) Certifications* [REDACTED]

---

<sup>6</sup> In this respect, section 702 appears to represent a departure from the "traditional" FISA framework, which expressly -- and significantly -- restricts the use of information acquired pursuant to surveillance activities authorized by the Attorney General without a court order and later rejected by the Court. *See, e.g.,* 50 U.S.C. § 1805(e)(5). ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED], *et al.*, Docket Nos. [REDACTED] Memorandum Opinion at 12 & n.11 (USFISC Oct. 3, 2011) (hereinafter "Oct. 3 Mem. Op."). Moreover, as the Government noted in its June 1 Submission, the Attorney General and Director of National Intelligence have confirmed that their prior section 702 authorizations continued to be valid and in force, notwithstanding the acquisition of Internet transactions featuring multiple discrete communications (hereinafter "MCTs"). *See* June 1 Submission at 35; *see also* Government's Response to the Court's Supplemental Questions of June 17, 2011, Docket Nos. [REDACTED], filed June 28, 2011, at 26-27. Accordingly, the Government respectfully submits that personnel who relied on those authorizations and followed those procedures in acquiring MCTs did not engage in unauthorized surveillance, and did not *intend* to engage in surveillance that was not authorized under FISA. ~~(TS//SI//NF)~~

2. The PAA ~~(S)~~

Section 105B of the PAA likewise empowered the Director of National Intelligence and the Attorney General to "authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States." § 105B, 121 Stat. at 552-55. Such acquisitions were specifically exempted from FISA's definition of "electronic surveillance." *See id.* § 105A, 121 Stat. 552. As under section 702, the PAA provided for judicial review of the targeting procedures used to implement those authorizations, but the review was limited by statute. Under

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

the PAA, the Attorney General was required to submit to this Court "the procedures by which the Government determines that acquisitions conducted pursuant to [its statutory authority] do not constitute electronic surveillance." *Id.* § 105C(a), 121 Stat. at 555. The Court, in turn, was then required to assess whether the Government's determination was "clearly erroneous." *Id.* § 105C(b), 121 Stat. at 555. As this Court has noted, the deferential "clearly erroneous" standard of review would "not entitle a reviewing court to reverse the [Attorney General's] finding . . . simply because [ . . . ] it would have decided the case differently." *In re DNI/AG 105B Certifications* [REDACTED] [REDACTED] Mem. Op. at 6 (USFISC Jan. 15, 2008) (hereinafter "PAA Mem. Op.") (quoting *Anderson v. City of Bessemer City*, 470 U.S. 564, 573 (1985)). Moreover, judicial review was limited to "certain aspects of the certification process." *Id.* at 4. "Executive branch determinations . . . regarding the purpose of the acquisition and the adequacy of minimization procedures [were] not subject to judicial review" at all. *Id.* at 6.

(TS//SI//NF)

Applying the PAA's "clearly erroneous" standard of review, this Court found the Government's targeting procedures were "reasonably designed to ensure that the users of tasked facilities are reasonably believed to be located outside the United States." *Id.* at 15. As to "abouts" communications, the Court "adopt[ed] the [Government's] interpretation that . . . surveillance [of 'abouts' communications] is 'directed' (i) at the users of tasked e-mail accounts . . . ; (ii) at those parties to acquired communications

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

who . . . are reasonably believed to be outside the United States; or (iii) at both these classes of persons." *Id.* at 21. Just as in the section 702 context, Government personnel who relied on the PAA authorizations to acquire MCTs did not engage in unauthorized surveillance, let alone did so intentionally. ~~(TS//SI//NF)~~

3. FISA Title I ~~(S)~~

The issues concerning NSA's upstream collection techniques raised during the Court's consideration of the above-captioned dockets potentially implicate the applications approved by the Court in *In re* [REDACTED]

[REDACTED] Docket Nos. [REDACTED]. ~~(TS//SI//NF)~~

With respect to Docket No. [REDACTED] the Government sought, and the Court approved, "authorization to direct electronic surveillance" at [REDACTED] that the Government believed were being used, or were about to be used, by its targets to communicate. In its order approving the surveillance, the Court stated that it "underst[ood] that, in certain instances, NSA may collect non-target [internet] communications." *In re* [REDACTED]

[REDACTED], Docket No. [REDACTED] Mem. Op. at 9 n.9 (USFISC Apr. 6, 2007) (hereinafter [REDACTED] Mem. Op."), just as the Court understood that "[a]lthough NSA surveillance will be designed to acquire only international [telephone] communications where one communicant is outside the United States, . . .

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

the manner in which [NSA] routes communications do not permit complete assurance that this will be the case," *id.* at 7-8 n.7. The Court approved the collection with the expectation that NSA would "handle these communications in accordance with its standard FISA minimization procedures, as described and modified herein." *Id.* at 9 n.9; see also *id.* at 7-8 n.7. Accordingly, Government personnel who relied on that approval and acted in accordance with those procedures in no way engaged in unauthorized surveillance, and certainly did not do so with "a conscious and objective desire to commit a violation." H.R. Rep. No. 95-1283, pt. 1, at 97 (1978) (quotation omitted).

~~(TS//SI//NF)~~

With respect to Docket No. [REDACTED] the Government acknowledges that its application did not fully explain the methodology through which [REDACTED] Internet communications upstream would "ensure that all communications forwarded to NSA . . . are indeed communications that have been sent or received using, and that 'refer to' or are 'about,' e-mail accounts/addresses/identifiers for which there is probable cause to believe are being used, or are about to be used, by [the targets.]" Decl. of Lt. Gen. Keith B. Alexander, Docket No. [REDACTED] filed May 23, 2007, at 21. But for the reasons discussed in greater detail above, this good faith mistake does not render the prior authorization void or the surveillance collected thereunder "unauthorized," thereby exposing Government personnel to potential criminal and civil liability. On the

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

contrary, such good faith mistakes can and should be meaningfully redressed without recourse to section 1809. ~~(TS//SI//NF)~~

II. Should the Court Determine that Unauthorized Collection Occurred, Only the Acquisition of Certain Subsets of Communications Acquired Through NSA's Upstream Collections Conducted Pursuant to the Authorities at Issue Would Constitute Electronic Surveillance, as Defined by the Act ~~(S)~~

By its terms section 1809(a) applies only to unauthorized electronic surveillance as that term is defined in FISA. Thus, the extent to which section 1809(a) applies to acquisitions under the authorities at issue herein depends on whether or not those acquisitions constitute "electronic surveillance." ~~(S)~~

NSA's upstream Internet collections under all four authorities have acquired only communications [REDACTED]

[REDACTED] As such, any communication that NSA has acquired through its upstream Internet collections conducted pursuant to the four authorities at issue would be a "wire communication," as defined by the Act -- that is, a "communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications." *Id.* § 1801(l). ~~(TS//SI//NF)~~

The Act defines "electronic surveillance" in four different ways. *See id.* § 1801(f).

Two of these four types of electronic surveillance on their face do not apply to NSA's upstream collections conducted pursuant to the authorities discussed in the Court's

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Briefing Order. The first type of electronic surveillance, which requires "intentionally targeting" a "particular, known United States person who is in the United States," *id.* § 1801(f)(1), is not implicated, because none of the authorities at issue here permitted the targeting of United States persons inside the United States.<sup>7</sup> Similarly, the third type of electronic surveillance, which involves the acquisition of the contents of certain radio communications, *see id.* § 1801(f)(3), is not implicated, [REDACTED]

[REDACTED] S)

For the reasons discussed below, the second type of electronic surveillance defined by the Act, which involves the acquisition of certain types of wire communications, *see id.* § 1801(f)(2), is potentially implicated to varying degrees (or not at all) in each of the four acquisition authorities at issue. *See, e.g., In re* [REDACTED]

[REDACTED]

[REDACTED], Docket No. [REDACTED] Application at 18-19, filed Dec. 13, 2006; *In re* [REDACTED]

<sup>7</sup> Specifically, in Docket No. [REDACTED], the authority granted by the Court required that "[a]ll selectors shall be telephone numbers or e-mail addresses that NSA reasonably believes are being used by persons outside the United States," *In re* [REDACTED]

[REDACTED] Docket No. [REDACTED] Primary Order at 12 (USFISC Apr. 6, 2007) (hereinafter "[REDACTED] Primary Order"); in Docket No. [REDACTED], the authority granted by the Court was "limited to the surveillance of telephone numbers and e-mail accounts/addresses/identifiers which the NSA reasonably believes are being used, or about to be used, by persons outside the United States," *In re* [REDACTED]

[REDACTED], Docket No. [REDACTED] Primary Order at 11 (USFISC Aug. 24, 2007) (hereinafter "[REDACTED] Primary Order"); under the PAA, the Government was only authorized to acquire "foreign intelligence information concerning persons reasonably believed to be located outside the United States," § 105B(a), 121 Stat. at 552; and under section 702, the Government may acquire foreign intelligence information through "the targeting of persons reasonably believed to be located outside the United States," 50 U.S.C. § 1881a(a), and is prohibited from "intentionally target[ing] any person known at the time of acquisition to be located in the United States," *id.* § 1881a(b)(1). (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

TOP SECRET//COMINT//ORCON,NOFORN

[REDACTED]

[REDACTED] Docket No. [REDACTED] Application at 16-17, filed May 24, 2007.<sup>8</sup> As noted above, all communications acquired through NSA's upstream collections under the four authorities are wire communications, as defined by the Act. Because the fourth type of electronic surveillance specifically excludes the acquisition of wire communications, *see id.* § 1801(f)(4), it does not apply to NSA's upstream collections under the authorities at issue. (TS//SI//NF)

Pursuant to the authority granted by this Court in Docket Nos. [REDACTED]

[REDACTED] NSA acquired wire communications through its upstream collections. To the extent that such wire communications (including any discrete communications within an MCT) were to or from a person inside the United States, the acquisition of those communications would have constituted electronic surveillance as defined in subsection 1801(f)(2). Most of that electronic surveillance was specifically contemplated and approved by the Court in these dockets. However, upon closer review of the record and as described below, certain wire communications to or from persons located in the United States acquired through NSA's upstream collections may not have been specifically contemplated by the Court at the time authorization orders were issued in Docket Nos. [REDACTED] (TS//SI//NF)

<sup>8</sup> [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] (TS//SI//NF)

TOP SECRET//COMINT//ORCON,NOFORN

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Section 105A of the PAA "carved out" of the FISA Title I definitions of electronic surveillance, a surveillance directed at a person reasonably believed to be located outside of the United States. § 105A, 121 Stat. at 552 ("Nothing in the definition of electronic surveillance under section 101(f) [i.e., 50 U.S.C. § 1801(f)] shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States."). As explained in detail below, NSA's acquisitions pursuant to the PAA were at all times the product of surveillance directed at persons reasonably believed to be located outside the United States and thus did not constitute electronic surveillance as defined by the Act. Accordingly, section 1809(a) is not implicated by NSA's acquisition of any communications pursuant to PAA -- even those that may not have been specifically contemplated or considered by the Court at the time it reviewed and approved NSA's targeting procedures as required by Section 105C of the PAA.<sup>9</sup>

~~(TS//SI//NF)~~

Unlike the PAA, section 702 did not exempt from the Act's definition of electronic surveillance the acquisitions contemplated by section 702. Many, if not most,

---

<sup>9</sup> As noted above, the scope of judicial review under the PAA was narrow. Section 105B(c) required the Attorney General to transmit to the Court a copy of each certification. *See* § 105B(c), 121 Stat. at 553. Section 105C(a) required the Attorney General to submit to the FISC "the procedures by which the Government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance." *Id.* § 105C(a), 121 Stat. at 555. Following such submission by the Attorney General, the Court was required to assess the Government's determination by applying a clearly erroneous standard. *See id.* § 105C(b), 121 Stat. at 555. Attorney General and Director of National Intelligence determinations regarding the purpose of the acquisitions and adequacy of the minimization procedures were not subject to Court review under Section 105C. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

of the wire communications NSA has acquired through its section 702 upstream collections were specifically contemplated and considered by the Court during its review and approval of NSA's targeting and minimization procedures as required by section 702(i) of the Act.<sup>10</sup> However, NSA has also collected certain other communications to or from persons located in the United States through its upstream collections pursuant to section 702 authorizations that were not specifically contemplated or considered by the Court at the time it reviewed and approved NSA's minimization and targeting procedures. ~~(TS//SI//NF)~~

For the reasons more particularly discussed above, the Government maintains that it did not engage in unauthorized electronic surveillance, let alone did so intentionally in violation of section 1809(a)(1). Should the Court determine that portions of the acquisitions under the four pertinent authorities were not authorized, the following summarizes the extent to which the Government believes section 1809(a)(2), which would govern the further disclosure or use of unauthorized acquisitions, would be implicated. For purposes of clarity and ease of understanding, this discussion categorizes the communications at issue in the same manner this Court

---

<sup>10</sup> Pursuant to section 702, the Court has jurisdiction to review certifications and minimization and targeting procedures and any amendments thereto. See 50 U.S.C. § 1881a(i)(1)(A). Certifications are reviewed to ensure that they contain all required elements. *Id.* § 1881a(i)(2)(A). Minimization procedures are reviewed to assess whether they meet the requirements of the Act and are consistent with the Fourth Amendment. *Id.* § 1881a(i)(2)(C). Targeting procedures are reviewed to assess whether they are reasonably designed to ensure that acquisitions are limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of wholly domestic communications. *Id.* § 1881a(i)(2)(B). ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

did in its opinion of October 3, 2011. In addition, as used in this discussion, the term "communication" refers to a single discrete communication within an Internet transaction.<sup>11</sup> ~~(S)~~

A. Active User is the Target ~~(S)~~

Under Docket Nos. [REDACTED] the PAA, and section 702, section 1809(a) is not implicated at all with respect to the acquisition of communications where the active user is the target. That is because such acquisitions were clearly authorized under all four authorities. *See, e.g., In re DNI/AG 702(g) Certifications* [REDACTED] *et al.*, Docket Nos. [REDACTED] Order at 3 (USFISC Oct. 3, 2011).<sup>12</sup> ~~(TS//SI//NF)~~

<sup>11</sup> An Internet transaction may consist of one or more single, discrete communications. *See* Oct. 3 Mem. Op. at 15. ~~(TS//SI//NF)~~

<sup>12</sup> The Government also notes that the acquisition of communications where the active user is the target in many cases does not constitute "electronic surveillance." With respect to Docket No. [REDACTED] Docket No. [REDACTED] and section 702, the acquisition of communications where the active user is the target constitutes electronic surveillance only to the extent that such communications are to or from a person in the United States. Under the PAA, the acquisition of all communications where the active user of the transaction is the target -- even communications to or from a person in the United States -- is not "electronic surveillance." As discussed above, the PAA removed from FISA's definition of electronic surveillance "surveillance directed at a person reasonably believed to be located outside of the United States." § 105A, 121 Stat. at 552. Where the active user of the acquired communication was the target, the surveillance resulting in that acquisition was directed at a person reasonably believed to be located outside the United States (i.e., the target). *See* PAA Mem. Op. at 13 ("[I]t is natural to think of the users of the tasked facilities as the persons at whom surveillance is 'directed.'"). Accordingly, such acquisitions are not "electronic surveillance" under the PAA. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

B. Active User is Not the Target and is Located Overseas ~~(S)~~

Under Docket No. [REDACTED] and section 702, the acquisition of communications where the active user of the communication is not the target but is located overseas potentially implicates section 1809(a), but only under very limited circumstances. First, section 1809(a) is not implicated if the communication of the non-target active user located outside the United States is to or from another person located outside the United States (including the user of a tasked selector), because the acquisition of such a communication is not "electronic surveillance."<sup>13</sup> Second, if the communication of the non-target active user located outside the United States is to or from a person located in the United States (and its acquisition is thus "electronic surveillance"), section 1809(a) is not implicated if the communication is one of the [REDACTED] types of "abouts" communications recognized by the Court in Docket No. [REDACTED] *see In re* [REDACTED], Primary Order at 13-14 (USFISC Aug. 24, 2007) (hereinafter "[REDACTED] Primary Order"); under the PAA, *see* PAA Mem. Op. at 17 n.18; and section 702, *see, e.g., In re DNI/AG Certification* [REDACTED], Docket No. 702(i)-08-01, Mem. Op. at 17-18 n.14 (USFISC Sept. 4, 2008) (hereinafter "[REDACTED] Mem. Op.").<sup>14</sup> It is only in cases where a communication of the

<sup>13</sup> Moreover, to the extent that such communications were to or from the user of a tasked selector (i.e., a target), the acquisition of such communications was authorized in any event. ~~(S)~~

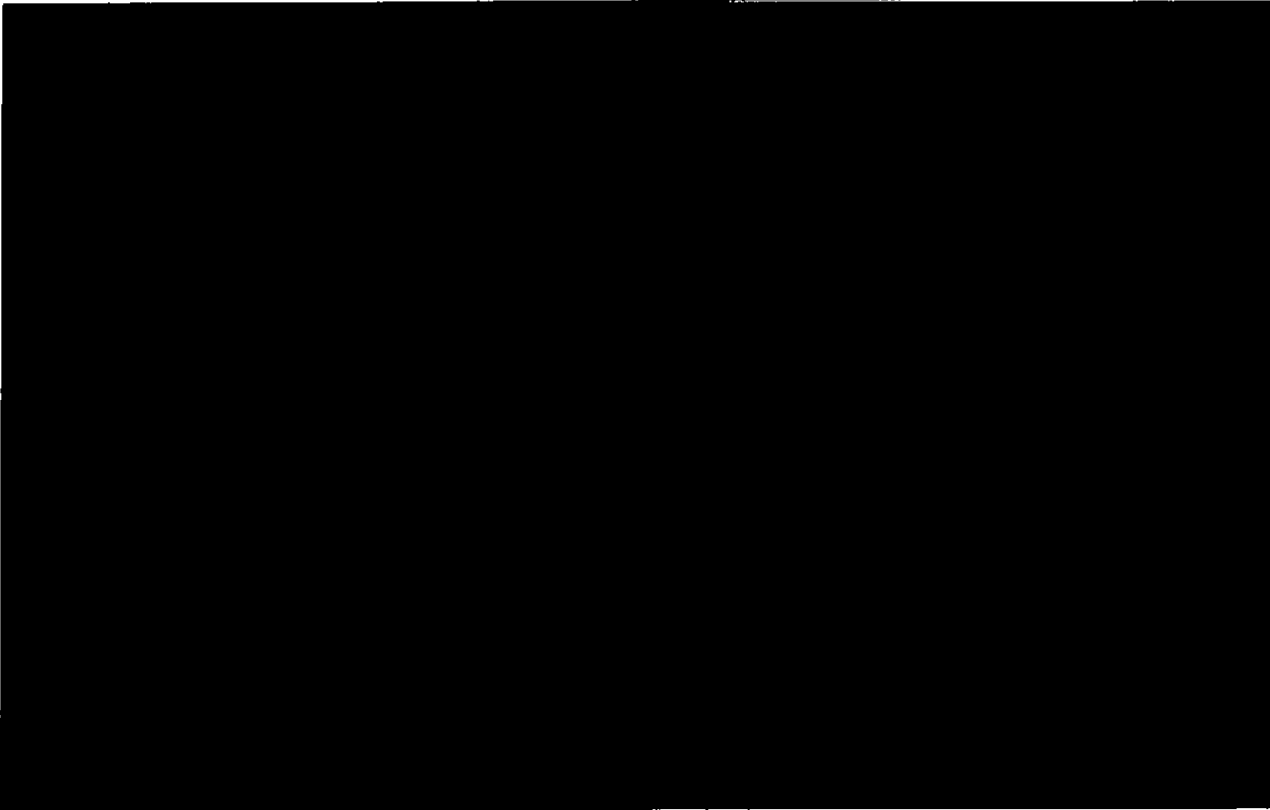
<sup>14</sup> For example, as explained by the Court in approving DNI/AG 702(g) Certification [REDACTED] the categories of "abouts" communications include where:

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

non-target active user outside the United States is (1) to or from a person located in the United States and (2) either is not one of the [REDACTED] types of "abouts" communications described to the Court, or the communication does not contain a tasked selector at all, that section 1809(a) is implicated by the acquisition of communications where the active user of the transaction is a non-targeted person located overseas. ~~(TS//SI//NF)~~

The acquisition of communications under Docket No. [REDACTED] where the active user of the transaction is not the target but is located overseas implicates section 1809(a) to an even lesser extent than similar acquisitions under Docket No. [REDACTED] and section 702. As with Docket No. [REDACTED] and section 702, the acquisition of a foreign-based

~~Id. (TS//SI//NF)~~~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

active user's communication does not implicate section 1809(a) if the communication is to or from another person located outside the United States (including the user of a tasked selector), because the communication is not acquired through "electronic surveillance."<sup>15</sup> Unlike Docket No. [REDACTED] and section 702, however, the scope of the acquisition of "abouts" communications was not defined under Docket No. [REDACTED] See [REDACTED] Primary Order at 8 n.6 ("The Court understands that [REDACTED] will select [REDACTED] not only international Internet communications to and from agents of [the targeted foreign powers], but also Internet communications in which e-mail addresses [REDACTED] or such agents are mentioned in the Internet communication."). Thus, if the communication of the non-target active user located outside the United States is to or from a person in the United States, its acquisition was authorized so long as a tasked selector was present in the communication, regardless of the type of "about" that communication is. It is only in cases where a tasked selector does not appear in a communication between a non-target active user located outside the United States and a person in the United States that section 1809(a) is implicated. ~~(TS//SI//NF)~~

Section 1809(a) is not implicated at all with respect to any communication acquired under the PAA where the active user of the communication is [REDACTED]  
[REDACTED]

---

<sup>15</sup> Again, to the extent that such communications were to or from the user of a tasked selector (i.e., a target), the acquisition of such communications was authorized in any event. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED] That is because all such acquisitions under the PAA resulted from surveillance directed at a person reasonably believed to be located outside the United States (i.e., the non-target active user). Specifically, if the communication is between [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>16</sup> The surveillance would also be directed at the non-target active user located outside the United States if the acquired communication was a communication sent to or from a person in the United States, even if the communication did not contain a tasked selector. Cf. PAA Mem. Op. at 21 (accepting, *inter alia*, that "abouts" surveillance is directed "at those parties to the acquired communications who, by virtue of the use of Internet Protocol filters or [REDACTED] [REDACTED] are reasonably believed to be located outside the United States."). Accordingly, such acquisitions do not implicate section 1809(a) because they do not constitute "electronic surveillance" as defined by FISA. ~~(TS//SI//NF)~~

C. Active User is Not the Target and Whose Location is Not (and Cannot Be) Known ~~(S)~~

Section 1809(a) is not implicated by acquisition under the PAA of *any* communications where the active user's location is not (and cannot be) known. This is

<sup>16</sup> The Government also notes that the acquisition of such a communication would not be "electronic surveillance" even in the absence of the § 105A carve-out, because the communication is not to or from a person in the United States. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

most evident when such communication is to or from a person located outside the United States (including the user of a tasked selector), at whom it can be said the surveillance resulting in the acquisition is directed. It is equally true, albeit somewhat counter-intuitively, for any communication between an active user whose location is not (and cannot be) known and a person located in the United States. As discussed above, section 105A of the PAA excluded surveillance that is directed at a person "reasonably believed" to be located outside the United States from FISA's definition of "electronic surveillance." The means described in the NSA's PAA targeting procedures -- i.e., the use of IP filters or [REDACTED] [REDACTED] -- operated to ensure that acquisitions were directed at a person reasonably believed to be located outside the United States. Just because NSA ultimately may be unable to determine the true location of the active user of the communication does not mean NSA did not reasonably believe, at the time of acquisition, that the surveillance was being directed at a person located outside the United States. Cf. *In re DNI/AG 105B Certifications* [REDACTED] Docket Nos. Transcript of Proceedings at 47-48 (USFISC Dec. 12, 2007) (hereinafter "PAA Transcript") (recognizing one possible scenario where [REDACTED]

[REDACTED]

[REDACTED] (TS//SI//NF)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Section 1809(a)(2) is also not implicated with respect to acquisitions under Docket No. [REDACTED], Docket No. [REDACTED] and section 702 where the communication is between a person outside the United States and an active user whose location is not (and cannot be) known. Section 1809(a)(2), which makes it a crime to intentionally "disclose[] or use[] information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this Act," among other authorities. If the location of the non-target active user cannot be determined, and the other communicant is known to be located outside the United States, then one cannot "know[] or hav[e] reason to know" that the communication was acquired through electronic surveillance at all. Cf. *In re* [REDACTED] *et al.*, Docket No. [REDACTED] Mem. Op. at 114 (USFISC [REDACTED] hereinafter "PR/TT Mem. Op.") (recognizing that "it might not be apparent from available information whether the communication to which a piece of data relates is to or from a person in the United States, such that acquisition constituted electronic surveillance as defined in Section 1801(f)(2)"). Section 1809(a)(2) can hardly be said to be implicated by the use or disclosure of communications acquired under such circumstances. *See id.* at 115 ("When it is not known, and there is no reason to know, that a piece of information was acquired through electronic surveillance not authorized by the Court's prior orders, the

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

information is not subject to the criminal prohibition in Section 1809(a)(2).").

~~(TS//SI//NF)~~

Under Docket No. [REDACTED] and section 702, it is only in cases where the active user is a non-target whose location is not (and cannot be) known communicates with a person in the United States that section 1809(a)(2) is potentially implicated. Yet if the communication of a non-target active user whose location is not (and cannot be) known is to or from a person in the United States, its acquisition under those two authorities does not implicate Section 1809(a)(2) if the acquired communication is one of the [REDACTED] types of "abouts" communications recognized by the Court. Under Docket No. [REDACTED] and section 702, it is only in cases where the communication is not one of these [REDACTED] types of "abouts" communications, or the communication does not contain a tasked selector at all, that 1809(a)(2) is implicated by the acquisition of a communication to or from a person in the United States where the location of the non-target active user is not (and cannot be) known. ~~(TS//SI//NF)~~

Acquisition under Docket No. [REDACTED] of communications to or from a person in the United States where the location of the non-target active user of the communication is not (and cannot be) known implicates section 1809(a)(2) to an even lesser extent than similar acquisitions under Docket No. [REDACTED] and section 702. That is because, as discussed above, the scope of the acquisition of "abouts" communications was not defined under Docket No. [REDACTED]. Thus, if the communication is between a non-target

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

active user whose location is not (and cannot be) known and a person in the United States, its acquisition was authorized so long as a tasked selector was present in the communication, regardless of the type of "about" that communication is. It is only in cases where a tasked selector does not appear in communication between a non-target active user whose location is not (and cannot be) known and a person in the United States that section 1809(a)(2) is implicated. ~~(TS//SI//NF)~~

D. Active User is Not the Target and is Located in the United States ~~(S)~~

Section 1809(a) is not implicated at all with respect to the acquisition of communications under the PAA where the active user is not the target and is located in the United States. Section 105A of the PAA excluded from the definition of "electronic surveillance" surveillance that is directed at a person reasonably believed to be located outside the United States. *See* § 105A, 121 Stat. at 552. As discussed in more detail below, communications acquired under the PAA where the active user was located in the United States -- even those that do not contain a tasked selector -- were the product of surveillance directed at a person reasonably believed to be located outside the United States, and thus did not constitute "electronic surveillance" by virtue of section 105A.

~~(TS//SI//NF)~~

This conclusion is most obvious where the communication is between a U.S.-based active user and the user of a tasked facility (i.e., the target). In that case, the surveillance is clearly directed at the foreign-based target. *See* PAA Mem. Op. at 13

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

("[I]t is natural to think of the users of the tasked facilities as the persons at whom surveillance is 'directed.'"). Somewhat less obvious, but no less true, are instances where the communication is between a U.S.-based active user and a non-target reasonably believed to be located outside the United States. Cf. PAA Mem. Op. at 21 (accepting, *inter alia*, that "abouts" surveillance is directed "at those parties to the acquired communications who, by virtue of the use of Internet Protocol filters or [REDACTED] [REDACTED] are reasonably believed to be located outside the United States."); *In re DNI/AG 105B Certification* [REDACTED] Ex. A (NSA Targeting Procedures), filed Aug. 17, 2007, at 1-2 ("In addition, in those cases where NSA seeks to acquire communications about the target that is not to or from the target, NSA will either employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas, or [REDACTED] [REDACTED]. In either event, NSA will direct surveillance at a party to the communication reasonably believed to be outside the United States.").

~~(TS//SI//NF)~~

Under the PAA, even the acquisition of communications that were in fact sent between an active user in the United States and another person in the United States did not constitute "electronic surveillance," so long as at the time of acquisition NSA reasonably believed that one of those communicants was located outside the United States. As discussed above, section 105A of the PAA excluded surveillance that is

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

directed at a person "reasonably believed" to be located outside the United States from FISA's definition of "electronic surveillance." The means described in the NSA's PAA targeting procedures -- i.e., the use of Internet Protocol (IP) filters or [REDACTED] [REDACTED] -- were reasonably designed to ensure that each acquisition was directed at a person reasonably believed to be located outside the United States.<sup>17</sup> That this reasonable belief may ultimately have proven to be mistaken does not mean that the acquisition resulted from "electronic surveillance" because the communication was in fact to or from a person in the United States. Cf. [REDACTED] Mem. Op. at 25 (concluding that "the government is authorized [under section 702] to acquire communications when it has a reasonable, but mistaken, belief that a target is a non-U.S. person located outside the United States"); PAA Transcript at 47-48 (recognizing one possible scenario where [REDACTED]

[REDACTED] [REDACTED]).<sup>18</sup> ~~(TS//SI//NF)~~

<sup>17</sup> As previously explained to the Court, these means are employed with respect to any Internet transaction acquired through NSA upstream collection, not just "abouts." See June 1 Submission, at 5. ~~(TS//SI//NF)~~

<sup>18</sup> The Court also concluded that "abouts" acquisitions were directed at the users of the tasked selectors referred to in those communications, rather than the senders or recipients of the communications. See PAA Mem. Op. at 21. Although this was not a theory advanced by the government, see *id.* at 20, the government notes that the acquisition of wholly domestic "abouts" communications would not be "electronic surveillance" under this theory either, because such surveillance would have been directed at the foreign-based user of the tasked selector. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Of course, section 1809(a) is potentially implicated under Docket No. [REDACTED] Docket No. [REDACTED] and section 702 in cases where the active user is located in the United States. That is because every such communication would be to or from a person in the United States (i.e., the U.S.-based active user) and, therefore, their acquisition would constitute electronic surveillance as defined in section 1801(f)(2). Thus, the relevant inquiry here focuses solely on whether such (f)(2) electronic surveillance was authorized. Most obviously, section 1809(a) is not implicated by the acquisition of communications between an active user in the United States and a user of a tasked selector, because such acquisitions would in all cases be authorized (f)(2) electronic surveillance. At the other end of the spectrum, the acquisition of the communications of a U.S.-based active user that do not contain a tasked selector implicates section 1809(a) if it is ultimately concluded that such acquisitions are not authorized. ~~(TS//SI//NF)~~

Falling between these two extremes is the acquisition of "abouts" communications of a U.S.-based active user. Under Docket No. [REDACTED], the acquisition of all types of "abouts" communications of a U.S.-based active user would be authorized (f)(2) electronic surveillance because, as discussed above, the scope of the acquisition of "abouts" communications was not defined under [REDACTED]. However, only those "abouts" communications of a U.S.-based active user that fall within the [REDACTED] types of "abouts" described to the Court under Docket No. [REDACTED] and section 702 would be authorized (f)(2) surveillance. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

As with the PAA, the acquisition of wholly domestic "abouts" communications under Docket Nos. [REDACTED] and [REDACTED] does not implicate section 1809(a). To acquire a communication under the authority granted in Docket No. [REDACTED] NSA was required to establish probable cause to believe that at least one party to the communication was outside the United States. See [REDACTED] Primary Order at 12. To establish this probable cause, NSA employed IP filters or [REDACTED]

[REDACTED] See *id.* at 8. Use of either of these means would "reasonably ensur[e] that the [acquired] communications originate or terminate in a foreign country." *Id.* That this probable cause determination may ultimately have been proven wrong in a particular case does not mean that the resulting acquisitions did not comport with the Court's order and thus were unauthorized. See, e.g., *Illinois v. Rodriguez*, 497 U.S. 177, 195 (1990) ("[T]he possibility of factual error is built into the probable cause standard."); *Illinois v. Gates*, 462 U.S. 213, 246 n.14 (1983) ("Probable cause . . . simply does not require [] perfection."). Indeed, this Court explicitly recognized that NSA's IP filters would not in all cases prevent the acquisition of all wholly domestic communications. See [REDACTED] Primary Order at 8 n.7 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~[REDACTED]"). ~~(TS//SI//NF)~~

The same holds true for the acquisition of wholly domestic "abouts" communications under Docket No. [REDACTED] Although the order entered in Docket No. [REDACTED] did not require NSA to establish probable cause to believe that a party to an acquired communication be located outside the United States, the Government's authority to acquire "abouts" communications under that docket was nonetheless limited to communications as to which "NSA reasonably believe[d] that the e-mail account/address/identifier [sending or receiving the 'abouts' communication was] being used, or [was] about to be used, by persons located outside the United States." [REDACTED] Primary Order at 15. The means approved by the Court for NSA to use to formulate that reasonable belief were the same [REDACTED] methods used under Docket No. [REDACTED]. See *id.* at 21 (recognizing that [REDACTED])

[REDACTED] IP filters may be used "to increase the chances of collecting foreign communications" and "to minimize acquisition of communications wholly within the United States."). Again, like under the PAA and Docket No. [REDACTED] the fact that these mechanisms did not in all cases prevent the acquisition of wholly domestic communications is not inconsistent with this reasonable belief; nor does it mean that an

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

acquisition conducted under that reasonable belief was unauthorized. *See, e.g.,*

*Rodriguez*, 497 U.S. at 195; *Gates*, 462 U.S. at 246 n.14. ~~(TS//SI//NF)~~

Section 1809(a) is implicated by the acquisition of "abouts" communications between a U.S.-based active user and another person in the United States under section 702. However, the Government notes that this Court recently held that NSA's targeting procedures are reasonably designed to prevent the acquisition of such communications, and that their acquisition does not run afoul of section 702(b)(4). *See* Oct. 3 Mem. Op. at 47-48. ~~(TS//SI//NF)~~

3. Whether the collections under Section 1881a, the PAA, and Docket Nos. [REDACTED] & [REDACTED] include information that was not authorized for acquisition, but is not subject to the criminal prohibitions of Section 1809(a). ~~(S)~~

Should the Court determine that NSA's upstream collection of communications that included "abouts" communications outside of the [REDACTED] categories previously specified to the Court in Docket No. [REDACTED], the PAA, and section 702,<sup>19</sup> as well as those discrete communications collected under all four pertinent authorities that are not to, from, or about a tasked selector, was not authorized, the Government believes that the following categories of information, although unauthorized, would not be subject to the provisions of section 1809(a), because they do not constitute electronic surveillance, as defined by FISA: ~~(TS//SI//NF)~~

---

<sup>19</sup> As noted above, the categories of "abouts" communications that could be acquired were not discussed or specified under the authorities granted in Docket No. [REDACTED] ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

(1) Where the active user is the target: As discussed above, where the active user is the target, all acquisitions were clearly authorized under all four authorities.

~~(TS//SI//NF)~~

(2) Where the active user is outside the United States or the active user's location is not (and cannot be) known: In such situations, acquisition would have been unauthorized, but would not have constituted electronic surveillance -- and therefore not subject to section 1809(a) -- in two situations, both of which would require the active user to be communicating [REDACTED]

[REDACTED]. First, under Docket No. [REDACTED], the PAA, and section 702, collection would be unauthorized where the acquired communication was about a tasked selector, but was not one of the [REDACTED] categories of "abouts" communications previously specified to the Court (*see footnote 14, supra*). Second, for all four authorities, collection would be unauthorized, but not subject to section 1809(a), where the discrete communication acquired (whether standing alone or within the context of an MCT) was not to, from, or about a tasked selector. ~~(TS//SI//NF)~~

(3) Where the active user is located inside the United States: As described above, due to the user's location in the United States, any unauthorized acquisition under Docket Nos. [REDACTED] and [REDACTED] as well as section 702 would constitute electronic surveillance as defined by 50 U.S.C. § 1801(f)(2), and therefore would be subject to section 1809(a). Acquisitions under the PAA, which as discussed

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

above were exempted from FISA's definition of electronic surveillance, would have been unauthorized, but not subject to section 1809(a), where (i) the acquired communication was about a tasked selector, but was not one of the [REDACTED] previously described categories of "abouts" communications, or (ii) where the acquired discrete communication (whether standing alone or within the context of an MCT) was not to, from, or about a tasked selector. ~~(TS//SI//NF)~~

**4. Whether any of the over-collected material has "aged off" NSA systems such that it is no longer retained by NSA or accessible to its analysts. ~~(S)~~**

As indicated above, NSA is implementing a reduced retention period of two years for upstream Internet collection from Docket Nos. [REDACTED] and [REDACTED], the PAA, and section 702, thus accelerating the scheduled age-off of such collection in NSA systems.<sup>20</sup> Doing so will require NSA to make significant adjustments to the software and handling rules associated with its repositories, and NSA estimates that it may take until at least March 2012 to responsibly complete the accelerated age-off without adversely affecting the data repositories and technical infrastructure NSA relies upon to appropriately handle the information it acquires pursuant to its section 702 authorities. NSA will update the Court on its progress at appropriate intervals and provide final notification once the accelerated age-off process has been completed.<sup>21</sup> The age-off will

---

<sup>20</sup> The two-year retention period will be calculated from the expiration of the relevant authorization. ~~(S)~~

<sup>21</sup> In the course of effecting the actions described herein, NSA may determine that it is necessary to submit amended procedures in response to operational concerns. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

result in a significant reduction in the amount of data that might contain information subject to section 1809(a)(2) should the Court determine that certain aspects of NSA's collection of Internet transactions upstream was not authorized. ~~(TS//SI//NF)~~

The material collected pursuant to Docket Nos. [REDACTED] and [REDACTED] DNI/AG 105B Certifications [REDACTED] under the PAA, and section 702 is subject to a five-year retention period, which is still in effect for all of these authorities. Accordingly, the oldest of the material is not due to begin to age off until 2012. However, as set forth above, NSA is currently in the process of applying an accelerated age-off to the upstream data collected pursuant to these authorities. ~~(TS//SI//NF)~~

As of the time of this filing, NSA has confirmed that unevaluated Internet transactions collected pursuant to PAA DNI/AG 105B Certification [REDACTED] [REDACTED] during the first twelve months it was in effect,<sup>22</sup> all of which featured a one-year retention period, has aged-off in NSA collection stores, corporate stores, [REDACTED] and some of NSA's backup systems. Thus, the data from [REDACTED] remains in certain NSA backup systems, but will eventually be removed.<sup>23</sup> [REDACTED]

<sup>22</sup> DNI/AG 105B Certification 08-01 [REDACTED]

[REDACTED] DNI/AG 105B Certification 08-01. ~~(S)~~

<sup>23</sup> NSA maintains backup and archive systems whose function is to provide data recovery in the event of a system failure or other disaster. The material which has not aged-off in the backup systems is not available for use by intelligence analysts. Because of the varied nature of the individual backup systems, NSA will assure compliance with the retention periods for collected data by requiring each system to

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED]

[REDACTED] However, as noted

above, the accelerated age-off process will remove the upstream data from DNI/AG 105B Certification 08-01 that is subject to the four-year extension, as well as Internet transactions collected pursuant to the PAA to the extent that those transactions had been evaluated, in whole or in part, and determined to be suitable for retention in accordance with the applicable minimization procedures. ~~(TS//SI//NF)~~

**5. If the government has determined that it has acquired information that is subject to Section 1809(a) or was otherwise unauthorized: ~~(S)~~**

- a. Describe how the government proposes to treat any portions of the prior unauthorized collection that are subject to the criminal prohibitions of Section 1809(a). ~~(S)~~**

As noted above, for technical reasons, NSA will not be able to apply retroactively the segregation process described in section 3(b)(5)a. of the 2011 Amended NSA Minimization Procedures to Internet transactions acquired via its upstream collection techniques prior to October 31, 2011. That data has already been distributed into NSA repositories. It would not be technically feasible for NSA to reach into those repositories and retroactively apply the segregation process described in section 3(b)(5)a. of the 2011 Amended NSA Minimization Procedures to data that is already within them. For that reason, and to further maintain consistency of its minimization

---

maintain the integrity of the age-off function through system requirements which will ensure that aged-off data is not reintroduced into collection, corporate, and/or analytic stores. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

procedures across acquisitions pursuant to multiple DNI/AG 702(g) certifications, NSA will train its analysts to conduct the analysis set out in section 3(b)(5)b. of the 2011 Amended NSA Minimization Procedures to all MCTs encountered by an analyst and make use of only those portions of an MCT authorized by section 3(b)(5)b. (TS//SI//NF)

Irrespective of the Court's final determination regarding the application of section 1809(a)(2), NSA fully intends to apply the requirements of sections 3(b)(5)(b) and 3(c)(2) of the 2011 Amended NSA Minimization Procedures to any use of Internet transactions previously collected through NSA's upstream collection techniques. Thus, NSA analysts will apply the applicable portions of the 2011 Amended NSA Minimization Procedures to all MCTs collected through NSA's upstream collection techniques prior to the Attorney General's adoption of the amended minimization procedures on October 31, 2011, and like all other upstream collection, information that does not meet the retention standards set forth in the amended procedures will only be retained for two years in any event. (TS//SI//NF)

**b. What steps is NSA taking to ensure that such information subject to 1809(a) is not used in proceedings before the Court?-(S)**

As reflected in the Government's Notice of Clarifications filed on August 30, 2011, NSA has implemented a process to review information from upstream Internet transactions prior to use in FISA applications or other submissions to this Court consistent with section 3(b)(5)b. in the 2011 Amended NSA Minimization Procedures.

See Notice of Clarifications, Docket Nos. [REDACTED] filed

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

August 30, 2011, at 9-10; *see also* 2011 Amended NSA Minimization Procedures, § 3(b)(5)b. NSA will work with the Department of Justice to implement the same process for any communications acquired pursuant to the four pertinent authorities when those communications are relied upon in a submission to this Court made by the Central Intelligence Agency (CIA) or Federal Bureau of Investigation (FBI). *See* 2011 Amended NSA Minimization Procedures, § 3(b)(5)b.<sup>24</sup> ~~(TS//SI//NF)~~

**c. What steps is the government taking to remediate any prior use of such information in proceedings before this Court. ~~(S)~~**

For all new applications to the Court that rely upon NSA information contained in a previous FISA application, the Government will ensure that information is subjected to the same process described above that is required by section 3(b)(5)b. of the 2011 Amended NSA Minimization Procedures. In particular, as noted above, NSA will work with the Department of Justice to implement that process for any communications acquired pursuant to the four pertinent authorities when those communications are relied upon in a submission to this Court made by CIA, FBI, or ~~NSA. (TS//SI//NF)~~

---

<sup>24</sup> As discussed in the 2011 Amended NSA Minimization Procedures, NSA analysts may not use communications that are not to, from, or about a tasked selector, but are to or from U.S. persons or persons located in the United States, except to "protect against an immediate threat to human life." *See* 2011 Amended NSA Minimization Procedures, § 3(b)(5)b.2.(c). Moreover, "if technically possible or reasonably feasible," NSA analysts will document their determination that a discrete communication not to, from, or about a tasked selector is to or from an identifiable U.S. person or person reasonably believed to be located in the United States. *See id.* To the extent that the minimization procedures allow for the use of discrete communications in an MCT, those discrete communications (including any U.S. person information contained therein) must be handled in accordance with the applicable provisions of the minimization procedures. *See id.* § 3(b)(5)b.2.(a) and (b). ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

- d. How does the government propose to treat any portions of the collection that are unauthorized but not subject to Section 1809(a), and explain why such treatment is appropriate. ~~(S)~~

This question necessarily encompasses two separate categories of information. Because section 1809(a)(2) only reaches the disclosure or use of information a person knows or has reason to know was obtained under color of law via unauthorized electronic surveillance as defined in section 1801(f) of FISA, the first category of information would include single, discrete communications within an MCT where NSA does not know, and has no reason to know, that such communication was acquired under color of law through electronic surveillance which was not authorized.<sup>25</sup> For example, and as described above, under certain circumstances when the communication is between a person outside the United States and an active user whose location is not (and cannot be) known, NSA may have no way to determine based on available information whether a single, discrete communication (or metadata extracted from that communication) was sent to or from a non-targeted person actually located in the United States such that the acquisition constituted electronic surveillance as defined

---

<sup>25</sup> This Court has previously concluded that section 1809(a)(2) does not criminalize all disclosures or uses of unauthorized electronic surveillance. Section 1809(a)(2) reaches disclosures or use only by a person "knowing or having reason to know that the information was obtained through" unauthorized electronic surveillance. 50 U.S.C. § 1809(a)(2). "When it is not known, and there is no reason to know, that a piece of information was acquired through electronic surveillance that was not authorized by the Court's prior orders, the information is not subject to the criminal prohibition in Section 1809(a)(2)." See PR/TT Mem. Op. at 115. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

by section 1801(f)(2).<sup>26</sup> The second category of information obviously would include single, discrete communications within an MCT which NSA knows or has reason to know were not acquired through unauthorized electronic surveillance. Such communications would include, for example, single, discrete communications within an MCT as to which the active user is a non-target who is reasonably believed to be located outside the United States [REDACTED]

[REDACTED] The Government does not believe that there should be any restriction on its ability to retain, access, or use these two categories of information consistent with the applicable portions of NSA's minimization procedures. ~~(TS//SI//NF)~~

Single, discrete communications within an MCT which do not contain the presence of a tasked selector (and which fall into one of the two categories set out above) may nevertheless contain foreign intelligence information which is relevant to the authorized purpose of the acquisitions conducted pursuant to the four relevant authorities, and NSA is required to limit its queries to those which are reasonably designed to return foreign intelligence information. *See, e.g.,* 2011 Amended NSA Minimization Procedures, § 3(b)(6). Moreover, as described above, NSA has committed to applying section 3(b)(5)b. of its amended section 702 minimization procedures to its

---

<sup>26</sup> While pointing out that the Government may not be willfully blind in assessing whether a piece of information was obtained through unauthorized electronic surveillance, the Court has previously found that "neither Section 1809(a)(2) nor any other provision of law precludes it from authorizing the government to access and use this category of information." PR/TT Mem. Op. at 115. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

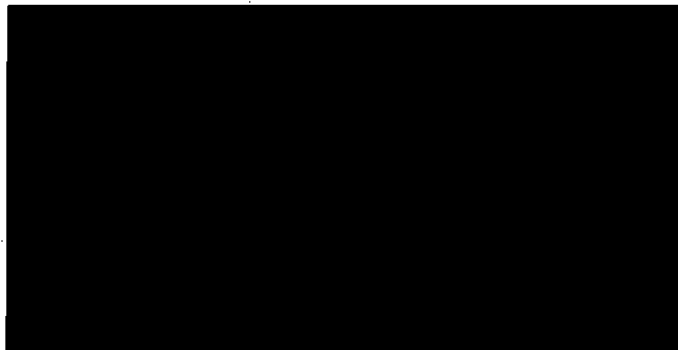
historical holdings, including transactions acquired pursuant to all four authorities at issue. Accordingly, even if the Court were to conclude that NSA's acquisition of certain information historically was not authorized, application of section 3(b)(5)b. of NSA's amended minimization procedures to its historical holdings would reasonably ensure that only information in MCTs which does not constitute electronic surveillance as defined by section 1801(f)(2) of FISA would be used or disseminated. ~~(TS//SI//NF)~~

6. Whether there are any other matters that should be brought to the Court's attention with regard to these collections that implicate Section 1809(a) or that were unauthorized. ~~(S)~~

After a thorough review of these collections, the Government has determined that there are no other matters that need to be brought to the Court's attention at this time that implicate section 1809(a) or that were unauthorized. ~~(S)~~

Respectfully submitted,

Tashina Gauhar  
Deputy Assistant Attorney General



National Security Division  
U.S. Department of Justice

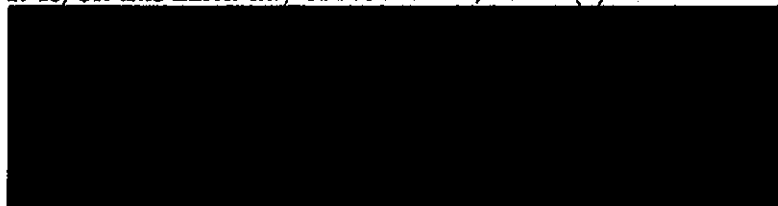
~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

VERIFICATION

I declare under penalty of perjury that the facts set forth in the attached Government's Response to the Court's Briefing Order of October 13, 2011, are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, § 1746, on this 22nd day of November, 2011. ~~(S)~~



Signals Intelligence Directorate Compliance Architect  
National Security Agency

~~TOP SECRET//COMINT//ORCON,NOFORN~~